THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF APPEALS

In re Application of:	)	
	)	Group Art Unit: 2133
Player et al.	)	
	)	Examiner: Esaw Abraham
Serial No. 10/037,959	)	
	)	Docket No.: applied_105
Filed: December 21, 2001	)	
	)	Customer No.: 29397
For: SYSTEM AND METHOD FOR	)	
GENERATING FORWARD	)	Confirmation No.: 7490
ERROR CORRECTION BASED	)	
ALARMS	)	
	)	

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

BRIEF ON APPEAL

This is an appeal from the rejection by Examiner Esaw Abraham, Group Art Unit 2133, of claims 1-22, all claims in the application, as set forth in APPENDIX A. The rejection was made in a Final Office Action dated December 3, 2004.

REAL PARTY IN INTEREST

The real party in interest is Applied Microcircuits Corporation, as assignee of the present application by an Assignment recorded in the United States Patent Office on December 21, 2001, at Reel 012449, Frame 0992.

RELATED APPEALS AND INTERFERENCES

None.

STATUS OF THE CLAIMS

Claims 1-22 are in the application.

Claims 1-22 are rejected.

Claims 1-22 are appealed.

STATUS OF AMENDMENTS

No claims have been amended.

SUMMARY OF THE INVENTION

Please refer to Fig. 1, and to the description at page 6, line 1 through page 7, line 7, for a general understanding of the system for generating forward error based alarms. A decoder 104 receives G.709 protocol data on line 106 encoded with forward error correction (FEC) bytes. The FEC bytes are overhead that accompany a message, permitting that message to be recovered even if some of the message bits are degraded. Thus, the FEC corrections are used to detect and correct errors in the

message. The error data is output on line 108. Alarm circuit 112 analyzes the detected errors and generates an alarm signal, on either line 114 or 116, in response to the analysis. Thus, the FEC corrections are indirectly used to generate an alarm signal if the number of errors corrected by the FEC process exceeds a predetermined error threshold.

THE ISSUES

1.   Whether Claims 1-22 are obvious under 35 U.S.C. 103(a) with respect to US Patent 6,487,686, Yamazaki et al. ("Yamazaki").

GROUPING OF CLAIMS

The claims are grouped as follows:

Claims 1-11 stand or fall together.

Claims 12-22 stand or fall together.

ARGUMENT AND DISCUSSION

Claims 1-22

The Final Office Action states that claims 1-22 are rejected under 35 U.S.C. 103(a) as being obvious with respect to Yamazaki. The Office Action states that Yamazaki teaches a receiver (59) that evaluates the error rate achieved by FEC checking B2 parity to correct errors and an error detector (5) that detects a *main* (emphasis added) signal error. As described below, a main error is generated when "even" parity is used with an "odd" number of bits. This error is also referred to as a mismatch. The Office Action states that receiver (59) generates an alarm in the occurrence of a *mismatch* (emphasis added). The Office Action acknowledges that Yamazaki does not explicitly teach a G.709 system, but

2

states that it would have been obvious to one of ordinary skill at the time of the invention to modify Yamazaki to include G.709 protocols.

MPEP § 2143 describes the three requirements needed to establish a *prima facie* case of obviousness.

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck* 947 F.2d 488, 20 USPQ2d, 1438 (Fed. Cir. 1991).

In his Background Section, Yamazaki describes the problem of using even parity FEC decoding to correct an odd number (3 or more) of bit errors. In this scenario, the FEC corrections may be improperly performed (col. 2, ln. 27-39). To address this problem, Yamazaki describes devices that communicate parity state information, to switch between states of valid and invalid FEC, which he calls "FEC states" (col. 6, ln. 62-65). It probably would have been less confusing if Yamazaki had termed these states as "parity states". More specifically, Yamazaki describes a system where the FEC states of a communicating transmitter and receiver must be the same. Yamazaki explains that if the receiver performs an FEC function when the transmitter is in an invalid FEC state (different parity), then the FEC corrections may be invalid (col. 7, ln. 1-10). "Thus, it is necessary to prevent such a *mismatch* (emphasis added) of FEC state between the transmission apparatuses. Additionally, it is necessary to detect such a *mismatch*..." (col. 7, ln. 17-20). To achieve this

3

goal, the transmitter stores its FEC state information in the overhead of a transmitted message (col. 7, ln. 43-45). Note, this "FEC state" data is not the same as the actual FEC bytes, which are also stored in overhead. The receiver derives the transmitter FEC state from the overhead, and compares its FEC state to the transmitter FEC state (col. 7, ln. 46-49). If there is a difference in FEC states, "the receiver may generate an alarm..." (col. 7. ln. 52-57). By properly switching FEC states, "it is possible to keep the *main* (emphasis added) signal from being erroneously changed." (col. 8, ln. 5-11).

Thus, Yamazaki's invention is enabled before the FEC bytes are actually read, or used to correct a message. As explained in detail below, Yamazaki's mismatch detection process is not the same as performing an analysis of FEC corrections, or using this analysis to generate alarm signals.

The invention of claims 1 and 12 describes the use of FEC bytes to detect errors, and the generation of error signals responsive to the detected errors. This process is a quantum improvement over the conventional G.709 Bit Interleaved Parity (BIP) process. With respect to the first *prima facie* requirement to support a case of obviousness, Yamazaki does not supply a suggestion to modify an FEC correction process in such a way as to generate an alarm signal. At col. 5, ln. 1-42, Yamazaki describes a conventional FEC process. However, Yamazaki does not suggest any analysis of the FEC corrections, or the generation of a signal in response to the number of errors that are detected. Further, Yamazaki does not describe a use for any such generated alarm signal. As described above, Yamazaki addresses the problem of a transmitter/receiver pair using a matching form of parity. This problem is

4

addressed by Yamazaki's invention prior to the actual use of the FEC bytes.

The fact that Yamazaki employs a receiver that decodes information using FEC corrections cannot, in and of itself, suggest a novel use of FEC correction data. In order for Yamazaki to make the invention of claims 1 and 12 obvious, there must be some suggestion in Yamazaki that FEC error data can additionally be used to generate communication alarm signals. Yamazaki describes an invention that insures that a communication transmitter and receiver use matching parity. But this matching parity system does not suggest a new FEC correction scheme or a novel use for FEC correction statistics.

Further, Yamazaki cannot lead to a reasonable expectation of success in the claimed invention, the second prong of the *prima facie* obviousness analysis. Although it may appear obvious in hindsight, there is no suggestion that a skilled practitioner, using Yamazaki as a reference, could reasonably be expected to come up with a device that provides alarm signals in response to using FEC bytes to detect errors in a received message.

An obviousness rejection based upon Yamazaki clearly fails in the analysis of third *prima facie* requirement. Yamazaki does not teach or suggest all the elements of the claimed invention. The claimed invention uses FEC bytes to detect errors, and generates an alarm signal in response to the detected errors. Yamazaki, however, detects "FEC states" from examining a message placed in overhead, and determines if the FEC states of a communicating transmitter and receiver are the same. If the FEC states are different, Yamazaki's receiver generates an alarm. Alternately stated, Yamazaki generates an alarm in response to a

5

mismatch between transmitter and receiver FEC states (parity states).
As noted above, Yamazaki determines the FEC state from examining an
overhead message, not from an analysis of errors that are corrected using
the FEC bytes. Once the receiver/transmitter FEC states are in synch,
conventional FEC corrections are preformed. Ultimately, Yamazaki does
not describe the limitations, from claims 1 and 12, of generating of an
alarm in response using FEC bytes to detect errors. Rather, Yamazaki
examines another message in overhead (not the actual FEC bytes) to
determine FEC state, and generates an alarm in response to a comparison
of FEC states. Claims 2-11, dependent from claim 1, and claims 13-22,
dependent from claim 12, also enjoy the above-mentioned distinctions
from the cited prior art. Yamazaki does not explicitly describe, or suggest
a modification that makes the claimed invention obvious.

In the **Response to the Applicant's Argument** Section of
the Final Office it states that "in figure 13 the prior art Yamazaki et al.
teaches or shows correspondences between results of the detection of the
mismatch (errors) and the switching operations of the FEC state of the
receiver and further the FEC function of the receiver is validated when
the FEC function is validated in both the transmitter and the receiver and
if there is a mismatch (an error) of the FEC state between the transmitter
and the receiver, an alarm is generated indicating the mismatch (see page
8, lines 29-37)."

The Examiner's analysis describes a relationship between
FEC state and receiver/transmitter communications. This analysis says
that an alarm is raised in the event of an FEC state mismatch. In other
words, an alarm is raised if the receiver is using a different type of parity
than the transmitter. This mismatch is an event that occurs, for example,

6

when even parity is used with a message containing an odd number of bits. This description clearly does not describe an alarm that is raised in response to an analysis of the errors that are detected in the FEC decoding process. Quite simply, once Yamazaki begins his FEC corrections, they are performed in an entirely conventional manner. Yamazaki's invention is enabled before the FEC corrections are actually made.
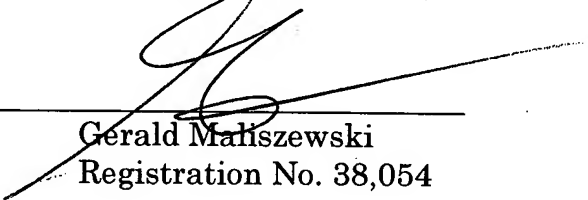
SUMMARY AND CONCLUSION

It is submitted that for the reasons pointed out above, the claims in the present application clearly and patentably distinguish over the cited reference. Accordingly, the Examiner should be reversed and ordered to pass the case to issue.

A check in the amount of $500.00 is enclosed to cover the fee for this Appeal Brief. Authorization is given to charge any deficit or credit any excess to Deposit Account No. 502033.

Respectfully submitted,

Date: December 16 2004

Gerald Maliszewski
Registration No. 38,054

Customer No.: 29397

APPENDIX A

1.   (Original)   In a G.709 network-connected integrated circuit, a method for generating alarms from forward error correction (FEC) data, the method comprising:

receiving messages including forward error correction bytes;

using the forward error correction bytes to detect errors in the messages; and,

generating alarm signals in response to the detected errors.

2.   (Original)   The method of claim 1 wherein using the forward error correction bytes to detect errors in the messages includes detecting a first number of errors; and,

wherein generating alarm signals in response to the detected errors includes generating a signal degrade (SD) signal in response to the first number of errors.

3.   (Original)   The method of claim 2 wherein using the forward error correction bytes to detect errors in the messages includes detecting a second number of errors, greater than the first number; and,

wherein generating alarm signals in response to the detected errors includes generating a signal fail (SF) signal in response to the second number of errors.

4.   (Original)   The method of claim 3 wherein generating an alarm signal in response to the detected errors includes generating a signal degrade (SD) signal in response to the first number of errors being detected within a first time period.

10

5.   (Original)   The method of claim 4 wherein generating alarm signals in response to the detected errors includes generating a signal fail (SF) signal in response to the second number of errors being detected within a second time period.

6.   (Original)   The method of claim 5 further comprising:

selecting the first number;

selecting the second number;

selecting the first time period; and

selecting the second time period.

7.   (Original)   The method of claim 6 further comprising:

selecting an error type; and,

wherein generating alarm signals in response to the detected errors includes generating an alarm signal in response to the selected error type.

8.   (Original)   The method of claim 7 wherein selecting an error type includes selecting a "1s" density alarm; and,

wherein generating alarm signals in response to the detected errors includes generating an alarm in response to the number of 1-bit errors detected.

9.   (Original)   The method of claim 7 wherein selecting an error type includes selecting a "0s" density alarm; and,

wherein generating alarm signals in response to the detected errors includes generating an alarm in response to the number of 0-bit errors detected.

10.　(Original)　The method of claim 7 wherein selecting an error type includes selecting a bytes density alarm; and,

wherein generating alarm signals in response to the detected errors includes generating an alarm in response to the number of byte errors detected.

11.　(Original)　The method of claim 7 wherein selecting an error type includes selecting a sub-row density alarm; and,

wherein generating an alarm signal in response to the detected errors includes generating an alarm in response to the number of sub-row errors detected.

12.　(Original)　In a G.709 network-connected integrated circuit, a system for generating alarms from forward error correction (FEC) data, the system comprising:

a forward error correction decoder having an input to receive messages including forward error correction bytes, the forward error correction decoder having an output to supply the number of detected errors in the messages; and,

an alarm circuit having an input to accept the number of detected errors and an output to supply alarm signals in response to the detected errors.

12

13. ·(Original) The system of claim 12 wherein the forward error correction decoder detects a first number of errors; and,

wherein the alarm circuit generates a signal degrade (SD) signal in response to the first number of errors.

14. (Original) The system of claim 13 wherein the forward error correction decoder detects a second number of errors, greater than the first number; and,

wherein the alarm circuit generates a signal fail (SF) signal in response to the second number of errors.

15. (Original) The system of claim 14 wherein the decoder has an output to supply a clock signal derived from the rate at which the messages are received; and,

wherein the alarm circuit has a input to accept the clock signal, and wherein the alarm circuit generates a signal degrade (SD) signal in response to the first number of errors being detected within a first time period of the clock signal.

16. (Original) The system of claim 15 wherein the alarm circuit generates a signal fail (SF) signal in response to the second number of errors being detected within a second time period of the clock signal.

17. (Original) The system of claim 16 wherein the alarm circuit has an input to select the first number, the second number, the first time period, and the second time period.

18.   (Original)   The system of claim 17 wherein the forward error correction decoder detects a plurality of error types; and,

wherein the alarm circuit has an input for selecting error type, and wherein the alarm circuit generates an alarm signal in response to the selected error type.

19.   (Original)   The system of claim 18 wherein the alarm circuit accepts a 1s density type error selection and generates an alarm in response to the number of 1-bit errors detected.

20.   (Original)   The system of claim 18 wherein the alarm circuit accepts a 0s density error type selection and generates an alarm in response to the number of 0-bit errors detected.

21.   (Original)   The system of claim 18 wherein the alarm circuit accepts a bytes density error type selection and generates an alarm in response to the number of byte errors detected.

22.   (Original)   The system of claim 18 wherein the alarm circuit accepts a sub-row density error type selection and generates an alarm in response to the number of sub-row errors detected.

APPENDIX B

TABLE OF CONTENTS